2020

More Amazon than Mafia: Analysing a DDoS stresser service as organised cybercrime

Roberto Musotto
Edith Cowan University

David S. Wall

10.1007/s12117-020-09397-5
Musotto, R., & Wall, D. S. (2020). More Amazon than Mafia: Analysing a DDoS stresser service as organised cybercrime. *Trends in Organized Crime*. Advance online publication. https://doi.org/10.1007/s12117-020-09397-5

Trends in Organized Crime
https://doi.org/10.1007/s12117-020-09397-5

More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime

Roberto Musotto[1] · David S. Wall[2]

Accepted: 5 October 2020/Published online: 04 November 2020

Abstract

The internet mafia trope has shaped our knowledge about organised crime groups online, yet the evidence is largely speculative and the logic often flawed. This paper adds to current knowledge by exploring the development, operation and demise of an online criminal group as a case study. In this article we analyse a DDoS (Distributed Denial of Service) stresser (also known as booter) which sells its services online to enable offenders to launch attacks. Using Social Network Analysis to explore the service operations and payment systems, our findings show a central business model that is similar to legitimate e-commerce websites in the way product, price and costumers are differentiated. It also illustrates that its organisation is distributed and not hierarchical and the overall income yield is comparatively low, requiring further organisational activity to make it pay. Finally, we show that the users of the service (mainly offenders) are not only a mixed group of actors, but that it is also possible to discriminate between different levels of seriousness of offending according to the particular service they purchased.

Keywords Organised crime groups online · Cybercrime · Organised crime · DDoS · Booter service · Stresser

This paper is based upon research conducted for the TAKEDOWN Project (Horizon 2020, Grant 700,688) and the ESRC Transnational Organised Crime (TNOC) research program. It also draws upon the work of the EPSRC CRITiCal project (EP/M020576/1). The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme. An earlier, though substantively different version of this research was published as Musotto and Wall (2019).

The opinions, findings and conclusions expressed in this article, however, are those of the authors and do not necessarily reflect those of the funding body.

✉ David S. Wall
d.s.wall@leeds.ac.uk

Roberto Musotto
R.Musotto@ecu.edu.au

[1] Cyber Security Cooperative Research Centre, School of Law, Edith Cowan University, Perth, Australia

[2] Centre for Criminal Justice Studies, School of Law, University of Leeds, Leeds LS2 9JT, UK

Introduction

There has been speculation for many years now in the cybersecurity community and press about the formation of internet mafias in the darkweb which have criminal or even terroristic intents (Bradley 2015, but also see McGuire 2012; Broadhurst et al. 2014; Lavorgna 2018). The organised crime trope and the internet is a recurring and powerful meme that has emotive strength as a statement but, arguably, does not stand up to scrutiny. Rather than clarify, it confuses existing differences in legal understandings of organised crime groups—which range from small ephemeral gatherings of career criminals to large international 'mafia ' organisations with clearly defined lines of command and control. This confusion perpetuates the "cyberpunk meets *The Godfather*" (Wall 2008: 872) theme and does not really leave researchers any-the-wiser. In this article we contribute to the broader debate about the nature of online crime groupings by exploring the logic of one crime group and its workings. Since mafias have specific characteristics, then we look for indications of these in this our analysis (also see further the discussion in Lavorgna 2018). Mafias traditionally facilitate crime and fear (Wu and Knoke 2017), whilst also organising and protecting the criminals under their wing through their powerful connections. The organised crime literature defines these as the 'who' of the criminal organisation (Paoli 2002), and they are qualitatively different to the 'what' of organised crime—the groups of online criminals who simply commit cybercrimes (Paoli and Vander Beken 2014; Von Lampe 2016). It is a subtle, but important difference. Whilst the speculation of their existence has been great, the evidence and indeed logic for such groups is less forthcoming and this article seeks to address this knowledge imbalance through the analysis of a case study.

Although, we have found in our research that most current online criminal organisations are very ephemeral in nature and are not sustainable in the longer term (see Musotto and Wall 2019) we anticipate, however, that this might change along with high impact cybercrimes such as Data Breaches,[1] Ransomware,[2] DDoS[3] (*Distributed Denial of Service)* and crimes of extortion and political revenge. These crimes are not only 'weaponising data', but they are also yielding large economic returns and therefore create a logic for a more sustainable (mafia) type model of crime group (see Musotto and Wall 2018). Such groups specifically seek to protect criminals and terrorists under their wing, invest their crime proceeds in the legitimate economy and/or in further spectacular attacks to increase their wealth, power and influence and ultimately their resilience and sustainability. As stated earlier, we believe that there is currently little evidence of such phenomena online on a large scale, although earlier findings have indicated that online organised crime groups are unlikely to imitate the more traditional forms of organised crime groupings. So, a key question to be answered later is do we 'park' the mafia model as a reference point to better understand online organised crime groups?

In this article we explore a specific form of cybercrime organisation (crimeware as a service) that is used to attack individuals, organisations or national infrastructure to disrupt their operations or even extort money. This idea is certainly not new because a

[1] Unauthorised intrusions to computer systems to exfiltrate data.
[2] Ransomwares is malicious software (*malware*) that, in their most basic form, prevents users getting access to data until a ransom is paid.
[3] DDoS attacks bombard access systems with login attempts to overwhelm them and prevent others accessing them.

criminal organisation, with an aspiring Mafia-type structure, thrives on dealing with social and economic interactions through the calculated use of violence and intimidation tactics. Technological advancement here is just an opportunity for creating new ways to shape such interactions and not an obstacle. Many studies, such as those by Cressey (1969); Kleemans and De Poot (2008); Van de Bunt et al. (2014); Brenner (2002); Kenney and Finckenauer (1995) describe the internal workings and structures of criminal organisations. Comparatively fewer studies, however, notably those by Kwitny (1979); Lupo (2018) and Sciarrone (2006), focus on the *social capital* that establishes and facilitates criminal organisations around the world. In an online setting, this social capital (criminal capital in the current context), translates into both the interest generated by (passive) offenders buying a product or service and using it for illicit consumption and also by (active) offenders buying a product or service and receiving support and protection whilst using it to carry out illicit activities. This study resonates with the market analysis and social network approach of those studies which analyse online criminal organisations and cryptomarkets (Leukfeldt et al. 2017; Munksgaard et al. 2019; Lusthaus 2018; Copeland et al. 2020). Our study, however, explores a different type of opportunistic product/service – the booter or stresser service, which can be hired and used to deliver illegal DDoS attacks. Booter service websites have already been studied by Hutchings and Clayton (2016) concerning motives of website operators and in the computer science field as characterisation and techniques to neutralise them (Krupp et al 2016, 2017; Santanna et al. 2016). Our paper adds knowledge by illustrating the challenges created by stresser services. We adopt social network analysis in order to understand the network and the relationship between DDoS users, services and revenues. This methodology highlights the specific behavioural pattern that purchasers show over time, allowing us to distinguish those who have a clear criminal intent from those who have not.

The first part looks at the ongoing debate over organised crime online. The second part analyses the technical aspects of DDoS stressers. The third part focuses upon an analysis of the StressSquadZ service (a pseudonym), forum and payments as a case study. The fourth part discusses the findings and identifies the offender groups from their consumption patterns and concludes.

The ongoing debate over organised crime online

Research into offline organised crime groups highlights a number of ways to understand the organisational structures of crime groups and their business models. We will summarise these to inform our later online case study. Albanese (2011), for example, suggests differentiating between the Hierarchical, Ethnic-Cultural and the Entrepreneurial Models of organised crime. *The Hierarchical Model* is found in traditional 'Mafia' organised crime structures and the more traditional terrorist groups, such as the IRA. The groups are organised according to a top-down leadership with one person (or controlling group) on top of pyramidal structure and many soldiers at the lower levels, with a number of levels of authority in between the levels. *The Ethnic/ Cultural Model* shares a common heritage that engages in both low-level and high-level crime to the benefit the entire group. Ethnic, Cultural or Religion ties bind the group together and individuals mostly control their own activities to achieve a common goal which may be

criminal or terror oriented. *The Enterprise model,* in contrast, differs from the hierarchical and ethnic/cultural models because the organised crime groups tend to operate more like legitimate business enterprises, but focus upon illicit instead of legitimate markets (Cornell 2006). They are rarely organised in a centrally structured way, rather, they operate along the same principles that govern legal markets, although they maintain and extend their share in illicit markets, thus responding to a variety of needs and demand on the part of their consumers. The aims of the groups falling within the organised crime enterprise model are mainly profit driven, and yet profit can be used to fund a terror campaign. We anticipate that our case study falls in this 'Enterprise' category, but with specific features that are more typical of online retailers. According to Hutchinson and O'Malley (2007) and also Makarenko (2004), cooperation between different groups is possible, but criminal organisations will never be able to identify themselves fully with terror groups because of the different purposes that drive them. This three-way differentiation is useful for delineating specific group orientations, even if—in practice—a combination of each of the models is likely, and also for identifying motivations. This differentiation is also an important guide when looking at our case study, which (spoiler alert), was purely 'enterprise' focused. It is therefore important now to differentiate between DDoS attacks, the attackers, and the stresser services that deliver them.

Our findings are consistent with those of Holt et al. (2012) who divided actors by skills and level of risk in order to find that there is only a small portion of online offenders who are highly skilled enough to pose an offending threat. Holt et al.'s research used demographic data collected through popular social network websites and blogs, while our dataset is a collection of transactions of an online community from a single website. Leukfeldt (2015) points out how similarities of cybercriminal organisations with Mafia groups could be the product of both mythology and the 'grey' cybersecurity literature, rather than the result of empirical academic research. Yet, structures in these multiple online organisations do exist as noted in multiple studies (e.g. Broadhurst et al. 2014; Dupont et al. 2017; Munksgaard et al. 2019) in that there are similarities in the ways that new members are selected or connect with each other. Plus, there are also cases where traditional Mafia-type organisations are seen to go online. Lavorgna and Sergi (2014) show how traditional offline criminal organisations have an opportunity online to profit from a lower risk environment in specific illicit markets such as online gambling. But these examples, tend to extend 'traditional' mafia fields of operation rather than explore 'new ground'.

Distributed denial of service (DDoS) attacks

Distributed Denial of Service (DDoS) tools have become very powerful over the years, especially when powered by cloud computing technologies (see Fig. 1). They have increasingly been used to attack systems with great effect. Their disruptive effect can either be used to cause reputational or business damage, or weaken security as a precursor to data theft, or they can be used to spread fear and even terror which causes uncertainties that can be leveraged to extort ransoms or influence change. DDoS attacks paralyse computer networks by flooding them with access data from various sources and blocking their access process, thus disrupting their operations. DDoS attacks slow

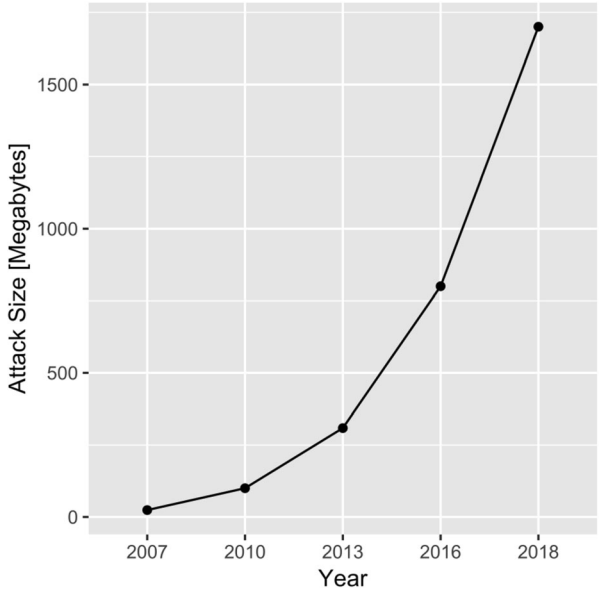

Fig. 1 Size of DDoS attacks over years. (Source: Morales 2018)

down or makes online services unavailable. In some cases, they can even make the system vulnerable to further attack, or theft of data, or for ransom. As stated earlier, they effectively 'weaponize data' and contribute to a new trend and level of criminal activity which seeks to disrupt business flows to extort gain. The impact of such attacks is ultimately economic or political, resulting in a loss of time and resources, but also loss of professional or economic reputation. DDoS can also create fear, if not a form of terror, when they disable infrastructures. Even resilience measures, which try to decrease potential disruption by installing larger servers to support heavier levels of traffic, or creating honeypot traps, or slow down and identify DDoS attacks and

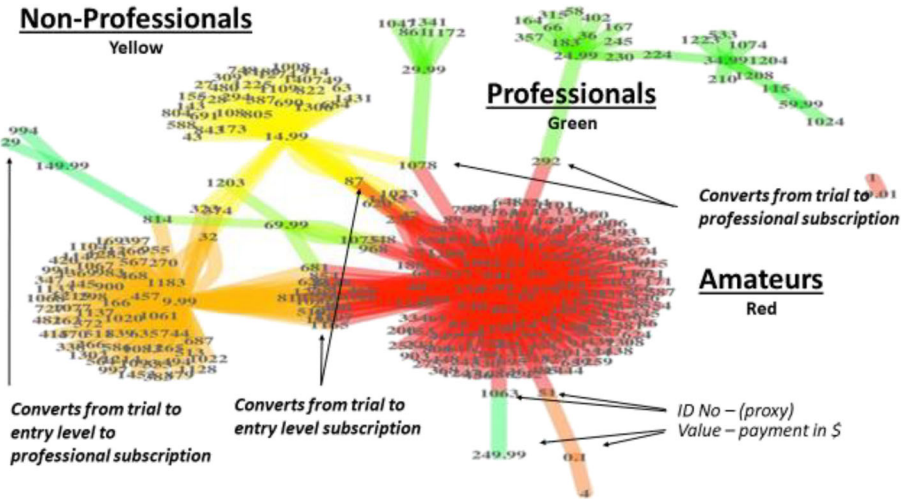

Fig. 2 The StressSquadZ network of users and plans bought with description

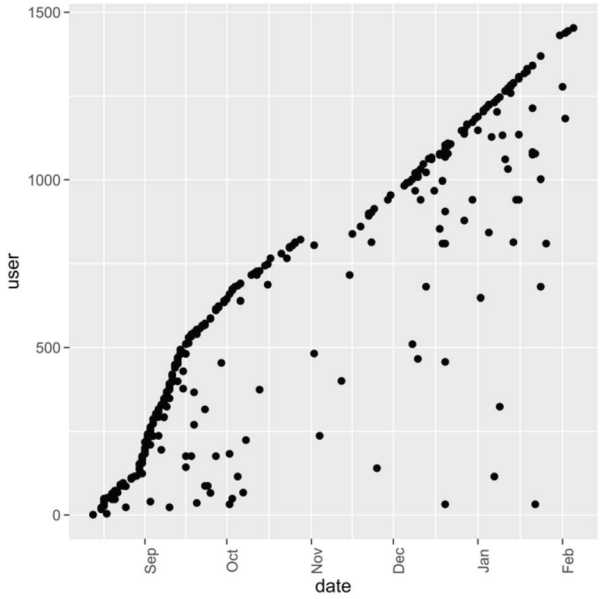

Fig. 3 Subscribing users and date of payments (n.b. taken down in February 2016). N.B. This graph shows how many people buy one of the products over time and how many of them repeat their purchase

malware entering a system network, are being challenged by an overall rise in the number of such attacks (Krupp et al. 2016). Morales (2018) illustrated this growth and found that, in 2007, the peak DDoS attack sizes were 24 megabytes. A decade later, in the first quarter of 2018, as shown in Fig. 1, the peak attack sizes had grown to 1.7 terabytes, almost a thousand-fold increase (Morales 2018). As the DDoS expands, new facilitating actors (DDoS brokers) are emerging who supply the tools, in exchange for a few dollars, pounds or bitcoins, for everyone to become a cybercriminal. Stressers are DDoS-for-hire services, a form of crimeware-as-a-service, usually sold via dark markets, to economic cyber actors, pranksters or hacktivists to prevent access to specific web sites. Distributed Denial of Service (DDoS) attacks are one of the most rapidly proliferating cybercrimes as they achieve a range of outcomes for offenders, although offender motivations and victims vary considerably. This raises the interesting question as to whether DDoS stressers also deliberately represent their organisation as a service to offenders, this marking the development of totally new criminal group online. Therefore, it is important to illustrate the ways that stressers can be utilised.

At the softer end of the DDoS attack spectrum, some DDoS attacks are simply intended to irritate or to test system security, or offenders are interested more in trying to impress friends or colleagues with their expertise than to cause serious damage. At the hard end of the spectrum, however, some attacks are clearly designed to inflict serious damage upon victim organisations, as in the alleged cases of cyberwarfare.[4] The attackers are motivated by the economic or political opportunities arising from that damage or disruption. Ponemon Institute, for example, found that the maximum cost of

[4] By cyberwarfare we intend the use of cybertools to disrupt the activities and the economic tissue of a State and its civil society.

an outage caused by DDoS more than doubled from $1 million in 2010 to more than $2.4 million in 2016 (Kassner 2016). In addition to financial loss, there are also examples of the way that DDoS attacks (launched from stressers) can be used in mixed crime-terror type situations.

One of the very first politically motivated cyber-attacks targeted Estonia in 2007 (Traynor 2007). With the interruption of internet communications and websites down, the spread of fake news undermining the Russian ethnic minority provoked rioting. In another example, a DDoS tool called the "Caliphate Cannon", was released in December 2016 in a deep web forum aligned with ISIS and institutional websites linked to the governments of Egypt, Iraq, Jordan and Yemen were targeted (Wolf 2017). Despite the evocative name, there was nothing terrifying about the 'Cannon', because it was quite weak due to the network structure supporting it.[5] Similar to the Estonia case, the 2017 DDoS attack on the Ukrainian postal service's (Ukrposhta) website (BBC 2017), shortly after a ransomware attack on the main strategic websites (allegedly by Russian criminals), provided examples of how these techniques can be used to achieve political goals. These typologies will be explored in greater detail in future publications, but in this article, we explore the structure of a main enabler of DDoS attacks, the stresser service.

Stresser services for hire to launch DDoS attacks?

What are stressers?

Stressers are semi-legal IT services, which for a fee, enable their clients to mobilise DDoS attacks. These can be legitimate when used to conduct legal and consensual penetration tests of computer systems to improve security. Improved security that could, for example, help companies and governmental organisations keep their websites afloat during heavy internet traffic. This is where a stresser can assist in developing resilience, so long as consent is given by the site owner. While stressers were created as testing tools, most are used to facilitate more malicious attacks. This potential semi-legitimate usage of stressers raises several important questions, for example, are they legally justifiable or are they just a hidden and dangerous form of crime-ware-as-a-service? Furthermore, to what extent does their organisational form illustrate new forms of organised crime online?

Stressers negotiate a peculiar position in a grey space, as both legitimate and illegitimate online service tools. For this research we analysed a data set taken from StressSquadZ (a pseudonym), a now defunct stresser (see Fig. 2) to see if it shares characteristics with offline criminal (and also terror) organisations, or even some well-known legitimate online service providers. In conducting this analysis, we also draw upon other recent cases and investigations such as Lizard Squad, Mirai malware. Using the data gathered from the StressSquadZ forum and analysing the activity of its members over a period of six months—from its opening to its takedown—we looked at the service provided, the users (clients) and also their transactions. We found that

[5] N.B. The Internet in Africa and Middle East has not the same internet speed than the Internet in Europe, Russia or the USA. Attacks launched from areas with poorer connections result in more limited and less effective disruptions. This lack of speed also raises doubts about the abilities and strategies of attackers, the DDoS malware in this case could have been a 'rebranding' or reuse of an existing tool.

most DDoS attacks had very low impacts in terms of damage caused and they also generated surprisingly small revenues, but this was set against almost non-existent risks in terms of being caught and a relatively small transaction window overall. The outcomes were also more complicated than expected because some uses had more serious consequences, which increased, the longer the services ran.

Stressers, as stated earlier, are largely used for illegal DDoS attacks. These are not only tolerated by stresser organisers, but also rarely prevented to the point that the lack of prevention is tantamount to an encouragement of abuse of service. For example, John Kelsey Gammell, an electronic technician from New Mexico, admitted to buying subscriptions for DDoS-for-hire services to launch attacks against businesses that had either fired or declined to rehire him. He also tried to recruit people with similar interests on social media to launch his own DDoS-for-hire service business (Claburn 2018). Business organisations and government agencies are usually the main targets of DDoS attacks, but the likes of gaming websites, for example, are also regularly affected as well by those seeking revenge for losses or financial gain by trying to interrupt the operating algorithms.

Many individuals, with an interest in IT, trial these attacks from a very young age and most are under the age of 20 (Hall 2016; NCA 2017). They pay for stressers to maliciously deploy software to launch DDoS attacks and they are often seemingly unaware of the broader consequences of their actions (Claburn 2018). See, for example, the case of Adam Mudd who created a malware called Titanium Stresser when he was only 15 years old and sold it online, He also used it to launch attacks upon websites, gamers and colleges. He allegedly profited from the malware by almost $400,000 and the Titanium Stresser was one that the Lizard Squad developed further for its own ends (Corfield 2017).

Once a stresser group forms, it is relatively easy for users to carry out successful attacks against bigger targets. This was the case with Lizard Squad which attacked Sony PlayStation, Xbox Live, Tor Network and Blizzards Warcraft (Amir 2018). The organisation of this group was extremely ephemeral in terms of its composition and activities, making it more difficult for law enforcement agencies not only to track down the individuals involved, but also to correctly prosecute them for their illicit actions. In fact, once such a group disappears following completion of a criminal activity, some of its surviving members will simply reform with others to create a new group, using their knowledge, and frustrating policing efforts. After multiple arrests of alleged members from online gangs, it appears that some continue to operate under a different name. For example, some of Lizard Squad appear to have reformed as BigBotPein, which released the Mirai malware and its variants in 2016 (Amir 2018). This is the same botnet used in August 2017 to attack and blackmail Lloyds Banking Group and Barclay's banks, infecting 1.25 million Deutsche Telekom routers (Schwartz 2017).

Because most stresser users seek a criminal goal, the providers are by default classed as an online organised crime group, especially as DDoS attacks are usually performed without the (victim) website owner's knowledge. Even though, the use of the site (facility) may often be justified on the grounds that it can be used for legitimate stresser testing (FBI 2017). Stressers create a cost to society (as mentioned earlier) by preventing access to businesses and disrupting their operations, with the effect of damaging their reputation in the market-place and reducing business and profit. They also create major challenges for law enforcement. In most jurisdictions, laws exist to

provide police and criminal justice systems with the powers to arrest, prosecute and imprison DDoS attackers, plus seize their computers and other electronic devices used as well as the proceeds of their crimes, which are also included within the investigative powers for cases of suspected terrorism or organised crime. The US Computer Fraud and Abuse Act (Sect. 18 U.S. Code 1030), for example and the UK Computer Misuse Act (1990 c.18) are legislative measures in two of many jurisdictions. But the laws focus upon the DDoS attackers, rather than those who actually facilitate the attacks—the brokers who operate the stressers (Porcedda and Wall 2019: 8). While DDoS attacks are hard to intercept quickly by law enforcers, it may, however, be possible to increase law enforcement powers to disrupt stressers when they are being used for criminal purposes and the link/ conspiracy between the stresser and attacker can be shown. Alternatively, introducing statutory regulations making providers ensure that they 'know their customers', or making sure that only approved payment systems are being used. Plus, also increasing the crime prevention mission by advising companies and governments to protect themselves by increasing their network bandwidth, multiplying their website providers, filtering out traffic, performing stress-tests, looking for spikes in traffic or avoiding using cryptocurrencies or PayPal when paying for a stresser. These measures could not only increase the security of targets but also potentially reduce the amount of damages and compensation paid by the company when the attack has not been prevented (Porter 2017). Also underlying these measures is a need to understand the nature of the stresser as crimeware-as-a-service and, to this end, we analyse a case study.

The StressSquadZ case study

We acquired anonymised forum data and website details from a stresser that had been taken down by law enforcement and shared with us by cybersecurity company DutchSec. Ethics approval was obtained during the realisation of the TAKEDOWN project.[6] The data we received had been already anonymised in order to prevent the actual identification of any user, plus, prior to this anonymisation, it must be pointed out that most of the original user IDs would have been proxies to preserve the users' initial identity (see Lusthaus 2018). Therefore, it would have not been possible for us to trace back users' actual identity as all identification details were either omitted, obscured or changed. The StressSquadZ website appeared to have been registered in multiple locations around the world under the name of the same owner.

We sought to understand how the stresser group was organised and used a social network analysis approach to explore the various types of service provided, the users and their transactions. Social network analysis is the most successful method for highlighting such group dynamics (Sparrow 1988) and is best suited to understand intra-group differences (Wolfer et al. 2015)—as in our case study. This methodology allowed us to analyse over 1400 users and visually outline their behavioural patterns. It is consistent with literature analysing large cohorts of people and offenders, and it allowed us to lay out similarities and differences in choices and interactions (Berlusconi 2013 and Carrington 2011). Moreover, it has already been used in the past for analysing online offenders (Holt et al. 2012).

[6] See further, Deliverable D2.2a of D2.2 of the TAKEDOWN project <https://www.takedownproject.eu/project-structure/>

In StressSquadZ, every user had a unique ID to access the website and forum. The same ID was used to carry out transactions. Therefore, when a user repeated a transaction the same ID would show up. We built a list of users transactions, outlining what they would buy, when and how many times. Each entry on the data would display a unique (anonymised) ID; the type of plan purchased; time and date of purchase. We built a separate list for the website forum where users would discuss their experiences of the stresser service. This second list contained more qualitative data as each entry would have an alphanumeric entry for the original poster in the forum; the title of the thread; the number of attacks carried by the original poster; the time and date of first thread; the thread moderator status for the original poster and the forum thread. It was not possible to integrate the two lists because the anonymised IDs were also randomised by the data supplier.[7] This is a limitation because the second list contained information that could have offered a better profile of the organisation, users and transactions, such as the number of attacks launched by each user. By comparing the two lists, however, it was still possible to infer that there were active and experienced users in the forum and that there were some users who spent considerable sums of money for the service, but it was not possible to pinpoint exactly who they were. One other limitation in this approach is that we had to assume that each ID is a different user, when some may also have had multiple profiles.

The list and data were processed with R software and *igraph* package. The graph chosen to represent the network employs a Fruchterman-Reingold algorithm (1991) as it allowed us to place similar nodes[8] closer to each other and distance different groups of users. In the graph from Fig. 2 peripheral nodes are the users. Each user is linked to a purchased plan, that, in the graph, is in a central position, as multiple users purchased the same service. We focused upon the payment plans and their take-up as it reveals much about the stresser's business model and operations (see Fig. 2 below).

Figure 2 is a visual representation of StressSquadZ in terms of its clientele and their payment plans. The offenders who hired the stresser were classified into three groups according to how much they paid for their services. The three categories of hacker grouping, the amateurs (wannabees and lamers), the skilled non-professionals (Hobbyists) and the Professionals, strongly align with groupings adapted from the 2006 Hacker Profiling Project (Chiesa et al. 2006; Porcedda and Wall 2019). They illustrate differential levels of usage in-line with different levels of skills and financial resources. It was assumed that the amateurs would be interested in the service if it was affordable, but not prepared to pay much for it as their intentions were driven more by curiosity. The skilled non-professionals would be prepared to pay more to achieve their aims, but not too much as they were not going to recover their costs. The professionals, by comparison, would be prepared to pay the most as they had high expectations of service and would expect a return on their investment.

StressSquadZ offered its clients various levels of service at different prices that ranged from the $1.99 trial to the $249.99 VIP (lifetime full power) service. A total of 359 payments were recorded and clustered according to the amount an individual paid. Each transaction was attached to a specific delivery plan, of which there were a total of 16. They started with trial plans and ended with premium VIP services. The payments

[7] Numeric and sequential in the payment list, alphanumeric in the forum list.
[8] Nodes in Social Network Analysis are generally the actors or the things in the network.

and subscription plans were found to be clustered around users and directed towards their chosen payment and subscription. Therefore, the users who picked the trial $1.99 plan (plan 1 in Table 1) were the majority – they paid 183 times. These are the red coloured links in the graph in Fig. 2. After the trial plans, the next popular category were the monthly subscriptions. Some users moved through different plans, say, from first choosing a trial plan to taking out a subscription plan. Seventy-three users upgraded their subscription from trial plans to monthly or even yearly or lifetime subscriptions. This is why it is possible to see multiple links emerging from users in Fig. 2. They are differently coloured according to the plan chosen and level of expertise.

The cheap trial plans did not allow users to perform full-power attacks and were limited in time, for example, they could do little more than temporarily reduce a fellow gamer's computer speed. That is the reason why we see in Fig. 2 some users who are tied to more than one plan. When their plans were checked with the timing of the payments it was possible to notice an evolutionary pattern from the trial service to lifetime subscriptions, suggesting a pathway into higher cost and more impactful plans. We also found that specific users displayed different consumer behaviour patterns. One user, for example, bought 5 trial plans, possibly because they were enough for his or her needs, rather than pay more for a more powerful service. In pure marketing terms, this technique attracts more people at a price set under or close to the actual cost of running the tool. They are effectively loss leaders which encourage subscribers to switch to a more expensive service. The majority of subscribers first bought a trial plan before buying a higher cost plan. Only 53 of the trial users did not upgrade to different plans. Please note that we consider that those who bought a trial plan either did not know how to use a stresser and tested it with the least economic effort possible, or they knew already how to use stressers, but did not know much about the StressSquadZ service. Yet, some of them clearly knew already how to use the service and managed to get a satisfactory result which encouraged them to upgrade to more a powerful

Table 1 Plans, subscriptions and offender groupings

Plan	Description of Plan	Plan Price	# Purchasers	Profits Generated	Offender Group
1	One off trial	$1.99	183	$364.17	Amateurs
16	Basic monthly	$9.99	87	$869.13	Skilled Non Professionals
2	3 Month subscription	$14.99	44	$659.56	Skilled Non Professionals
3	Quarterly	$24.99	15	$374.85	Skilled Non Professionals
3	Quarterly	$29.99	5	$149.95	Skilled Non Professionals
4	Monthly full-power	$34.99	8	$279.92	Skilled Non Professionals
23	3 month full-power	$59.99	3	$179.97	Professionals
6/5	Quarterly full-power	$69.99	7	$489.83	Professionals
13/20	Yearly full-power	$149.99	3	$449.70	Professionals
10	VIP Service Lifetime full-power	$249.99	1	$249.99	Professionals
		Total	359	$4,067.28	All

N.B. The plan numbers were assigned by StressSquadZ and changed during its lifetime

subscription. We interpret this result from the number of attacks launched by these users and the fact that after the trial, they bought the plan more than once.

Some clients, in contrast, never upgraded because the service did not suit their needs, or they did not possess the skills to run an attack (e.g. the amateurs). Hence this is why not every user in the red area is not also linked to other plans. Furthermore, there were also users who knew how to run stressers very well and needed a powerful service that was strong enough to take down larger complex websites. These users paid the highest prices for the higher-grade services and in some cases, received a bespoke service. In Fig. 2, these are coloured in yellow (skilled non-professionals) and green (for professionals, the top-level users). This finding was obtained by comparing the quantitative data with the qualitative data from the forum analysis. More experienced users sought to buy a tailored service with features that beginners did not have access to. Another observation was that not all the users in the discussion forum made purchases or subscribed to plans and there was a relatively low level of engagement. Only 285 users (out of 1451) were subscribers to trials or other plans. This observation was also reflected in the wider crime forum literature (see, for example, Karami et al. 2016). We interpret this finding in terms of the interest being generated about the service as only the buyers focus upon their engagement and activity. Users joined the club because they heard about it in other forums or from other users and they were curious about its capabilities. This was apparent from the forum threads, which in this case study were structured in a help-desk format, in which the most active members posted at least four threads.

Profits

When we explored how much profit the stresser generated, we found a figure of $4067.28 per month at its peak. This is actually a low profit margin compared to that generated by other stresser groups – but probably still a lot of money to a young person. The VSO stresser, for example, is reported to have made $24,737 profit per month and Lizard stresser around $6,000 per month (Karami et al. 2016). The income of StressSquadZ may, however, have been smaller than the others because of its relatively short operating period and take up. Figure 3 shows that many users bought a plan at the launch of the service, but take-up slowed down before then stopping almost completely in November when only 5 members renewed their subscription with no new users joining. Could this have been because other stresser services were taking away the business? In December and January new subscription and renewals began again at a steady pace. It is also possible to see that, with the exception of a few cases, renewals took place a short time after the initial purchase (this is noticeable in Fig. 3 by looking at the dots that fall under the line).

Once we matched this finding with the price paid by users over time (see Fig. 4), it was found that higher prices were paid straight away at the first purchase, suggesting that this group (e.g. skilled non-professionals and professionals) were composed of experienced users, who already possessed a set of skills necessary to use the tools. Analysis of the prices paid indicate the existence of at least two groups, the amateurs (or wannabees) and the skilled non-professionals. The early birds and users who bought the service after November spent the most money, while between those two sets were few renewals and many trial subscriptions.

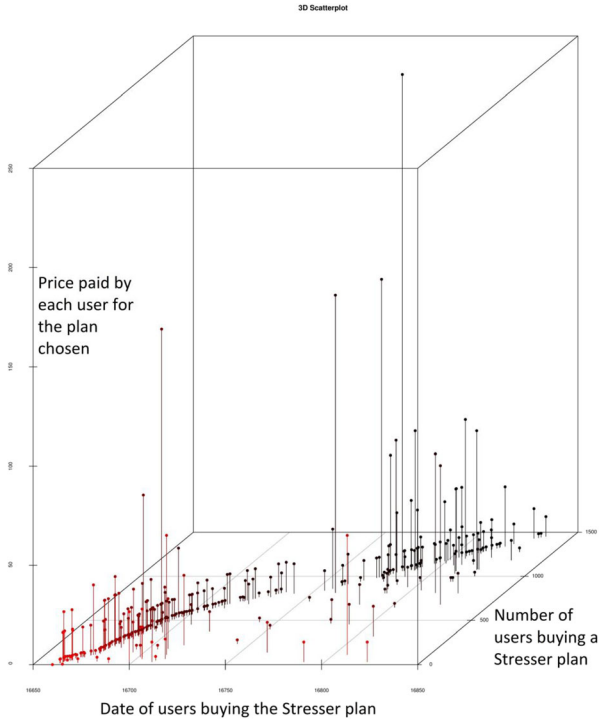

Fig. 4 3D graph showing subscribing users, date of payments and price paid

User activities

An analysis of member's activity and their payment patterns shows that not everyone who subscribed to StressSquadZ could have had an active interest in performing a DDoS attack. Alternatively, they may not have wanted to pay to carry one out or they may have simply been curious? In the forum thread, only 127 of the 1451 (9%) members actively appear to have carried out an attack.

Organisation and customer support

Furthermore, it seems that whilst there was only one owner of the forum and two members with administrative powers, another sixteen members were very active in replying to forum threads and launching attacks, thus, playing a central role in delivering the stresser. There was also a customer service section that helped clients with their queries but also protected and maintained the stresser. Table 2 shows the list of the users who opened more threads in the forum. It was not possible to match the payment data of some users with their forum threads, but the forum data did provide some useful information on tracking down members who posted payment details on threads – it is not shown here, as it could possibly reveal the identity of the people involved with such activities (although most identifiers were themselves proxies).

Table 2 Most active users in the ticket forum (N.B. Names are pseudonyms)

User	Threads Open
Zoukie100	14
WantuxModz	13
Xxxxxxx1	7
Zanne2	6
B832348208	6
Kaonimade	5
Quubaa78	4
Dlipstick	4
XilenXD1	4

Discussion and conclusion: identifying offending groups from consumption patterns

The main use of StressSquadZ, as indicated earlier, was mainly without the consent of the website owner (the legal grounds for its takedown) and since this constitutes a crime, then companies or groups (because some are not formally registered as companies) providing stressers are effectively a new form of online organised crime grouping. One solution to reduce DDoS cyber-attacks would be to automatically close down all stresser service providers, however, the effectiveness of such an action is not as straightforward as often assumed. When Webstresser.org, a large Stresser provider, was shut down by authorities in April 2018 (Kunert 2018), DDoS attacks reduced by 60 per cent (Cimpanu 2018). This large reduction was, however, only temporary, because the void created by the takedown was quickly filled by new entrants in the market. In the least case scenario, members and customers of online services such as stressers satisfy their intellectual curiosity without ever consciously causing damage. In the worst-case scenario, they give malicious individuals a justification for their criminal actions, especially creating fear and terror. This line of thought not only challenges the more simplistic assumptions about DDoS attacks, but also the potential for expanding the crime/terror/fear nexus, with the implication that the division between organised crime and terrorism is becoming increasingly blurred. Technology, in brief, relentlessly alters the features of crime and terror as opportunities and demand arise.

There were many similarities between the way the stresser was provided and how the online retailers of legal products and services work. This can be noticed in three innovative aspects. Their service differentiation marketing strategy, for example, helped them expand the market and acquire new users and user groups. As observed earlier, StressSquadZ offered a trial period to quickly grab the market and get users acquainted with the service. It also provided higher levels of service and client interaction for those with advanced skills and needs. This enabled this second group to look for a best buy and it attracted users who are usually extremely inelastic in their behaviour, and (from what we saw) tend to get more support from the ticket support service.[9] Our analysis of the differential marketing strategy clearly demarcated between three offender groups that were indicated earlier.

[9] Ticket service is an issue tracking system, where a service desk organises all the problems that arise with products into a specific workflow to get a solution in the most efficient way.

First, there were the 'amateurs' (red in Fig. 2), *ingénue* who mainly bought the service out of curiosity to try it out, often after becoming interested following discussions in other chat forums. Sometimes they did not really know how to use the service properly or wished to try it out of curiosity or to commit small or unique attacks and then stop. These, we argue, were not particularly seriously minded offenders and probably either regarded their use of the stresser as part of a hobby, or as a way of improving their computing skills (e.g. wannabees and script-kiddies), possibly not even realising the illegality of using it. As the offending intent in their action is lower, when compared to other offenders, education about the impact of cybercrime would help to address their behaviour.

The 'amateurs' contrasted with a second group, the 'skilled non-professionals' who constituted more serious offenders. These are the users with orange and yellow links in Fig. 2. These 'skilled non-professionals' knew exactly which kind of service they were after, perhaps because of previous experience and/or their advanced skills. Moreover, they understood how a stresser works and were clearly shopping around for the best value for money. Once they had tried a stresser out under the trial scheme and were happy with it, a number upgraded their plan to the VIP service. These are the groups of people who have the required skillset to carry out organised crime and even terror attacks.

A third category of stresser users was the 'professional' (green in Fig. 2). Like a sponsored athlete or racing driver who advertises powerful cars, they show to potential users what can be done with the service. They not only demonstrate its potential but also give the illusion of its power, effectiveness and efficiency – what it can do for the user. But, like the sports industry, the supply of high-end products and services is limited, the cost is high and to use a specific product implies that the user needs specific characteristics or features, which not everyone possesses. These are the individuals who also expose the stresser sites to broader audiences and markets, but in time, also to law enforcement agencies.

Different criminal actors use stressers to achieve different crime outcomes and each group played a different role in the business model of StressSquadZ's differential marketing strategy in terms of attracting different amounts of revenue. Whilst the amateurs constituted half (51%) of payments, they only reflected a tenth (10%) of the total sums received. The skilled non-professionals, on the other hand, constituted two fifths (43%) of payments, but provided about half of the total profits. The professionals constituted a much smaller percentage (6%) of the market share, but two fifths (41%) of all profits, as shown in Table 1. This observation suggests the importance of website takedowns where there is a clear legal case to do so. The indication here is that stressers (cybercrime-as-a-service) may not always be as lucrative as it is often made out to be, there was a surprisingly low yield which contrasted against expectations. Yet it is likely if StressSquadZ had been allowed to mature into a larger business then the profits would have been all the much greater, not only encouraging the offending group who formed it but also educating them as to where 'the money is!'.

The findings of this research are not as dramatic as the tropes, rhetoric and cultural hype surrounding organised crime would suggest, which reflects the broader contrast between media expectations and reality (see further, Collier et al. 2020). Yet, StressSquadZ was nevertheless a facilitator of DDoS attacks which can have very serious long-term consequences for victims and it was one of a number of similar services. There was little evidence that StressSquadZ (or any other stresser) was ever used to deliberately produce the sort of terror shock that a kinetic explosion would. There was equally little evidence of Stresser

services producing the large fear backlash that ultimately shapes the political process. The problem is that in terms of wider 'policing' priorities the impact of this sort of cybercrime doesn't "bang, bleed or shout" (Officer cited by Dearden 2019) and so, does not create the panic that demands instant response from, and funding for, police agencies. Yet, although this stresser may have appeared to be a fairly low level, it, like many others, could launch as large an attack as the offender's resources would permit.

In conclusion, our analysis indicates there was a clear organisation of the market, which does not resemble the 'classical' model described in the literature (see, for example, Gambetta and Reuter 1995). It also showed that organised cybercriminals, like many other offending groups online, are adaptive and seek to balance the maximisation of profits (the proceeds of their crime) with the minimisation of operating risks (including arrest and prosecution). The relatively low yield and focus on 'making it work' also indicated that intellectual motivation was as important as economic success (though with the earlier caveat that its takedown denied the service the opportunity to mature). In this way StressSquadZ was not a hierarchical organisational structure, more a distributed form (Wall 2015) but operated along quite fundamental business principles and looked, as our title indicates, more like Amazon than the Mafia.

Compliance with ethical standards

Please note that this research was conducted following a successful application for ethical approval from University of Leeds.

Conflicts of interest There are no potential conflicts of interest.

Research involving human participants and/or animals The research does not directly involve human participants. The data was anonymised when received and doubly anonymised so that any possible identifiers have been substituted by proxies.

Informed consent No animals were involved in this research.

References

Albanese JS (2011) Transnational crime and the 21st century: Criminal enterprise, corruption, and opportunity. Oxford University Press

Amir W (2018) Lizard Squad is alive and continuing activities as BigBotPein: Report, HackRead, 31 January. https://www.hackread.com/lizard-squad-is-alive-continuing-activities-as-bigbotpein/ (visited on 03/15/2018)

BBC (2017) Ukranian postal service hit by 48-hour cyber attack. BBC News Online, 10 August. https://www.bbc.co.uk/news/technology-40886418 (visited on 03/15/2018)

Berlusconi G (2013) Do all the pieces matter? Assessing the reliability of law enforcement data sources for the network analysis of wire taps. Global Crime 14(1):61–81

Bradley T (2015) Cybercrime Is The Modern-Day Mafia. Forbes. 16 October. Available at https://www.forbes.com/sites/tonybradley/2015/10/16/cybercrime-is-the-modern-day-mafia/ (visited on 09/04/2020)

Brenner SW (2002) Organized cybercrime-how cyberspace may affect the structure of criminal relationships. NCJL & Tech 4:1

Broadhurst R, Grabosky P, Alazab M, Bouhours B, Chon S (2014) Organizations and Cybercrime: An analysis of the nature of groups engaged in cyber crime. Int J Cyber Criminol 8(1):1–20

Carrington PJ (2011) Crime and social network analysis.The SAGE handbook of social network analysis, 236–255

Chiesa R, Ducci S, Ciappi S (2006) H.P.P. The hacker profiling project: A General overview, paper to the hack.lu 2006 conference, 19- 21 October, Luxembourg

Cimpanu C (2018) DDoS attacks go down 60% across Europe following WebStresser's Takedown, BleepingComputer, 2 May. https://www.bleepingcomputer.com/news/security/ddos-attacks-go-down-60-percent-across-europe-following-webstressers-takedown/. Visited on 15 March 2018

Claburn T (2018) Sad-sack Anon calling himself 'Mr Cunnilingus' online is busted for DDoSing ex-bosses, The Register, 18 January. https://www.theregister.co.uk/2018/01/18/it_technician_ddos_former_employer/ (visited on 03/15/2018)

Collier B, Clayton R, Hutchings, Thomas D (2020) Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies. Workshop on the Economics of Information Security. https://www.cl.cam.ac.uk/~bjc63/Crime_is_boring.pdf. Visited on 15 July 2020

Copeland C, Wallin M, Holt TJ (2020) Assessing the practices and products of Darkweb Firearm vendors. Deviant Behav 41(8):949–968

Corfield G (2017) Brit behind titanium stresser DDoS malware sent to chokey, The register, 25 April. https://www.theregister.co.uk/2017/04/25/british_malware_author_2_years_jail_titanium_stresser/ (visited on 03/15/2018)

Cornell SE (2006) The narcotics threat in greater Central Asia: from crime-terror nexus to state infiltration? China Eurasia Forum Q 4(1):37–67

Cressey DR (1969) Theft of the nation: the structure and operations of organized crime in America (Vol. 174). Transaction Publishers

Dearden L (2019) British public left at risk of fraud because it is 'not police priority', watchdog finds. The Independent, 2 April. https://www.independent.co.uk/news/uk/crime/fraud-uk-police-watchdog-scam-priority-funding-cuts-a8849956.html. Visited on 31 Mar 2020

Dupont B, Côté AM, Boutin JI, Fernandez J (2017) Darkode: Recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world." Am BehavSci 61(11):1219–1243

FBI (2017) Booter and stresser services increase the scale and frequency of distributed denial of service attacks: Alert Number I-101717b-PSA, FBI Public Service Announcement, 17 October. https://www.ic3.gov/ media/2017/171017–2.aspx (visited on 03/15/2018)

FruchtermanReingold TMEM (1991) Graph drawing by force-directed placement. SoftwPractExp 21(11): 1129–1164

Gambetta D, Reuter P (1995) Conspiracy among the many: the mafia in legitimate industries. In The economic dimensions of crime (pp. 99–120) Palgrave Macmillan, London

Hall K (2016) DDoS script kiddies are also... actual kiddies, Europol arrests reveal, The Register, 12 December. https://www.theregister.co.uk/2016/12/12/europol_arrests_34_ddos_kiddies/ (visited on 03/15/2018)

Holt TJ, Strumsky D, Smirnova O, Kilger M (2012) Examining the social networks of malware writers and hackers. Int J Cyber Criminol 6(1):891–903

Hutchings A, Clayton R (2016) Exploring the provision of online booter services. Deviant Behav 37(10): 1163–1178

Hutchinson S, O'Malley P (2007) A crime–terror nexus? Thinking on some of the links between terrorism and criminality. Studies in conflict terrorism 30(12):1095–1107

Karami M, Park Y, McCoy D (2016) Stress testing the booters: Understanding and undermining the business of DDoS services. In: Proceedings of the 25th International Conference on World Wide Web. International World Wide Web Conferences Steering Committee, 1033–1043.https://doi.org/10.1145/2872427.2883004

Kassner M (2016) The rising cost of DDoS. Data Center Dynamics Magazine, 22 April. https://www.datacenterdynamics.com/analysis/the-rising-cost-of-ddos/. Visited on 31 Mar 2020

Kenney DJ, Finckenauer JO (1995) Organized crime in America. Wadsworth, Belmont, p 341

Kleemans ER, De Poot CJ (2008) Criminal careers in organized crime and social opportunity structure. Eur. J. Criminol 5(1):69–98

Krupp J, Backes M, Rossow C (2016) Identifying the scan and attack infrastructures behind amplification DDoS attacks. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 1426–1437 https://doi.org/10.1145/2976749.2978293

Krupp J, Karami M, Rossow C, McCoy D and Backes M (2017) Linking amplification DDoS attacks to booter services. In International Symposium on Research in Attacks, Intrusions, and Defenses (pp. 427–449). Springer, Cham

Kunert P (2018) Webstresser.org taken down by Europol plod and chums. 25th of April. https://www.theregister.co.uk/2018/04/25/worlds_biggest_ddosforhire_site_shuttered_admins_cuffed/(visited on 25/10/2018)

Kwitny J (1979) Vicious Circles: The mafia in the marketplace. WW Norton & Company Incorporated

Lavorgna A (2018) cyber-organised crime. A case of moral panic?,trends in organized crime, https://doi.org/10.1007/s12117-018-9342-y

Lavorgna A, Sergi A (2014) Types of organised crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of Internet technologies. International Journal of Law, Crime and Justice, 42(1), 16–32

Leukfeldt ER (2015) Organised cybercrime and social opportunity structures: A proposal for future research directions. The European Rev of Org Crime 2(2):91–103

Leukfeldt ER, Kleemans ER, Stol WP (2017) Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. Br J Criminol 57(3):704–722

Lupo S (2018) La Mafia. DonzelliEditore, Rome

Lusthaus J (2018) Industry of Anonymity: Inside the Business of Cybercrime. Harvard University Press, Cambridge, Mass

Makarenko T (2004) The crime-terror continuum: tracing the interplay between transnational organised crime and terrorism. Global crime 6(1):129–145

McGuire M (2012) Organised crime in the digital age. John Grieve Centre for Policing and Security and BAE Systems Detica

Morales C (2018) NETSCOUT arbor confirms 1.7 Tbps DDoS attack; The terabit attack era is upon us, Arbor networks, 5 March. https://www.arbornetworks.com/blog/asert/netscout-arbor-confirms-1-7-tbps-ddos-attack-terabit-attack-era-upon-us/(visited on 03/15/2018)

Munksgaard R, Décary-Hétu D, Mousseau V and Malm, A (2019) Diversification of tobacco traffickers on cryptomarkets. Trends in Organized Crime, 1–22.

Musotto R, Wall DS (2018) Are Booter Services (Stressers) indicative of a new form of organised crime group online? UNODC Linking Organized Crime and Cybercrime Conference, School of Global Studies, Hallym University, Chucheon, South Korea, 7–8 June 2018

Musotto R, Wall DS (2019) The online crime-terror nexus: using booster services (stressers) to weaponise data? In: Ruggiero V (ed) Organised crime and terror networks, Ch 4. Routledge

NCA (2017) Pathways into cyber crime.National Crime Agency. https://www.nationalcrimeagency.gov.uk/publications/791-pathways-into-cyber-crime/file (visited on 03/15/2018)

Paoli L (2002) The paradoxes of organized crime. Crime Law Soc Chang 37(1):51–97

Paoli L, and Vander Beken, T (2014) Organized crime: A contested concept. In The Oxford handbook of organized crime (pp. 13–31). Oxford University Press.

Porcedda MG, Wall DS (2019) Cascade and chain effects in big data cybercrime: Lessons from the TalkTalk hack. In: Proceedings of WACCO 2019: 1st workshop on attackers and cyber-crime operations. IEEE EuroS&P 2019, Stockholm, Sweden, June 20, 2019 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3429958

Porter D (2017) How localgovs can guard against DDOS stresser attacks, EfficientGov, 15 November. https://efficientgov.com/blog/2017/11/15/how-localgovs-guard-against-DDOS-stresser-attacks/ (visited on 03/15/2018)

Santanna JJ, Schmidt RDO, Tuncer D, De Vries J, Granville LZ and Pras A (2016) Booter blacklist: Unveiling DDoS-for-hire websites. In 2016 12th International Conference on Network and Service Management (CNSM) (pp. 144–152). IEEE

Schwartz MJ (2017) Daniel Kaye charged With DDoS, blackmail against Lloyds and Barclays Banks, Information Security Media Group. 31 August. https://goo.gl/3vh9Ds (visited on 03/15/2018)

R Sciarrone (2006) Nodi, intrecci, connessioni: il potere delle reti mafiose. In L. Pepino et M. Nebiolo (eds.), Mafia e potere. Turin: Edizioni Gruppo Abele

Scott J (1988) Social network analysis. Sociology 22(1):109–127

Traynor I (2007) Russia accused of unleashing cyberwar to disable Estonia. The Guardian. 17 May. https://www.theguardian.com/world/2007/may/17/topstories3.russia (visited on 03/15/2018)

Van de Bunt H, Siegel D, and Zaitch D (2014) The social embeddedness of organized crime. In The Oxford handbook of organized crime (pp. 13–31). Oxford University Press

von Lampe K (2016) The ties that bind: a taxonomy of associational criminal structures. In Illegal Entrepreneurship, Organized Crime and Social Control (pp. 19–35). Springer, Cham

Wall DS (2008) Cybercrime and the culture of fear: social science fiction and the production of knowledge about cybercrime. Inf Commun Soc 11(6):861–884. Revised in May 2010. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1155155

Wall DS (2015) Dis-organized crime: Towards a distributed model of the organization of cybercrime. The European Review of Organised Crime 2(2):71–90

Wolf K (2017) Cyber Jihadists Dabble in DDoS: Assessing the threat. Flashpoint. July 13. https://www.flashpoint-intel.com/blog/cyber-jihadists-ddos/ (visited on 03/15/2018)

Wölfer R, Faber NS, Hewstone M (2015) Social network analysis in the science of groups: Cross-sectional and longitudinal applications for studying intra-and intergroup behavior. Group Dyn Theory Res Pract 19(1):45

Wu M, Knoke D (2017) Dark Networks: The Terror-Crime Nexus. Palgrave Handbook of Inter-Organizational Relations in World Politics. Palgrave Macmillan, London, pp 471–484